PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32

A1

(11) International Publication Number: WO 99/26373

(43) International Publication Date: 27 May 1999 (27.05.99)

(21) International Application Number: PCT/US98/23328

(22) International Filing Date: 2 November 1998 (02.11.98)

(30) Priority Data:
08/971,157 14 November 1997 (14.11.97) US

(71) Applicant *(for all designated States except US)*: DIGITAL PERSONA, INC. [US/US]; Suite 226, 805 Veterans Boulevard, Redwood City, CA 94063 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BJORN, Vance [US/US]; 431 Clifton Avenue, San Carlos, CA 94070 (US). RIGHI, Fabio [IT/US]; 157 Burns Avenue, Atherton, CA 94027 (US).

(74) Agents: SALTER, James, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

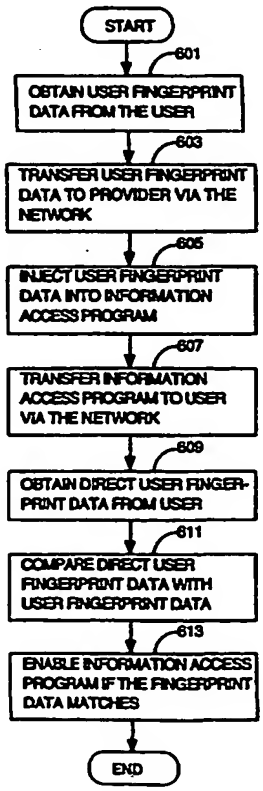
(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: METHOD FOR USING FINGERPRINTS TO DISTRIBUTE INFORMATION OVER A NETWORK

(57) Abstract

A method, apparatus, and article of manufacture for distributing information from a provider to a user over a network. User fingerprint data is obtained from the user (601) and transferred to the provider via the network (603). The provider injects the user fingerprint data into an information access program (605) and transfers the information access program back to the user via the network (607). Direct user fingerprint data is then obtained from the user (609) and compared to the injected user fingerprint data (611). If there is a match, the user is enabled to use the information access program (613).



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | |
|---|---|
| AL | Albania |
| AM | Armenia |
| AT | Austria |
| AU | Australia |
| AZ | Azerbaijan |
| BA | Bosnia and Herzegovina |
| BB | Barbados |
| BE | Belgium |
| BF | Burkina Faso |
| BG | Bulgaria |
| BJ | Benin |
| BR | Brazil |
| BY | Belarus |
| CA | Canada |
| CF | Central African Republic |
| CG | Congo |
| CH | Switzerland |
| CI | Côte d'Ivoire |
| CM | Cameroon |
| CN | China |
| CU | Cuba |
| CZ | Czech Republic |
| DE | Germany |
| DK | Denmark |
| EE | Estonia |
| ES | Spain |
| FI | Finland |
| FR | France |
| GA | Gabon |
| GB | United Kingdom |
| GE | Georgia |
| GH | Ghana |
| GN | Guinea |
| GR | Greece |
| HU | Hungary |
| IE | Ireland |
| IL | Israel |
| IS | Iceland |
| IT | Italy |
| JP | Japan |
| KE | Kenya |
| KG | Kyrgyzstan |
| KP | Democratic People's Republic of Korea |
| KR | Republic of Korea |
| KZ | Kazakstan |
| LC | Saint Lucia |
| LI | Liechtenstein |
| LK | Sri Lanka |
| LR | Liberia |
| LS | Lesotho |
| LT | Lithuania |
| LU | Luxembourg |
| LV | Latvia |
| MC | Monaco |
| MD | Republic of Moldova |
| MG | Madagascar |
| MK | The former Yugoslav Republic of Macedonia |
| ML | Mali |
| MN | Mongolia |
| MR | Mauritania |
| MW | Malawi |
| MX | Mexico |
| NE | Niger |
| NL | Netherlands |
| NO | Norway |
| NZ | New Zealand |
| PL | Poland |
| PT | Portugal |
| RO | Romania |
| RU | Russian Federation |
| SD | Sudan |
| SE | Sweden |
| SG | Singapore |
| SI | Slovenia |
| SK | Slovakia |
| SN | Senegal |
| SZ | Swaziland |
| TD | Chad |
| TG | Togo |
| TJ | Tajikistan |
| TM | Turkmenistan |
| TR | Turkey |
| TT | Trinidad and Tobago |
| UA | Ukraine |
| UG | Uganda |
| US | United States of America |
| UZ | Uzbekistan |
| VN | Viet Nam |
| YU | Yugoslavia |
| ZW | Zimbabwe |

# METHOD FOR USING FINGERPRINTS TO DISTRIBUTE INFORMATION OVER A NETWORK

## FIELD OF THE INVENTION

This invention relates generally to a fingerprint comparison system, and more particularly to a method for using fingerprints to distribute information over a network.

## BACKGROUND OF THE INVENTION

Securing computer systems and electronic transactions is becoming more and more important as we enter the electronic age. Existing password and cryptographic techniques seem well on their way to solving the security problems of computer systems, electronic commerce, and electronic transactions. These solutions ensure that the set of digital identification keys associated with an individual person can safely carry on electronic transactions and information exchanges. Little, however, has been done to ensure that such identification keys can only be used by their legitimate owners. This is a critical link that needs to be made secure if secure computer access, electronic commerce, home banking, point of sale, electronic transactions, and similar mechanisms are to become truly secure.

Today, passwords handle most of these issues. For example, most electronic transactions, such as logging into computer systems, getting money out of automatic teller machines, processing debit cards, electronic banking, and similar transactions require passwords. Passwords are an imperfect solution because as more and more systems attempt to become secure, a user is required to memorize an ever expanding list of passwords. Additionally, passwords are relatively easily obtained by

observing an individual when he or she is entering the password. Moreover, there is no guarantee that users will not communicate passwords to one another, lose passwords, or have them stolen. Thus, passwords are not considered sufficiently secure for many functions.

More and more often, fingerprint identification is considered. Fingerprints have the advantage of being unique to an individual person, requiring no memorization, and being relatively difficult to appropriate. Thus, some secure systems are switching to fingerprint recognition. Fingerprint recognition generally requires a user to place his or her finger on a fingerprint sensing device. Each fingerprint consists of a unique arrangement of ridges and grooves. The fingerprint sensing device transmits an analog image of the user's fingerprint, via a coaxial cable, to a computer system. The computer system then matches the fingerprint to a database of fingerprint templates in the computer system.

Public access information networks, such as the Internet, are being used to distribute a wide variety of information. However, public networks such as the Internet are not secure and there is a danger of information being copied or intentionally misrouted as it is being transmitted. Further, transmitted information, if it is protected at all, is usually protected by a traditional password scheme which is not able to verify that the person using the password is authorized to do so. Therefore, there is a need for a secure way to distribute information over a network which protects against possible information copying or misrouting and which can verify that only an authorized user can access the information.

## SUMMARY OF THE INVENTION

The present invention provides a method, apparatus, and article of manufacture for distributing information from a provider to a user over a network. User fingerprint data is obtained from the user and transferred to the provider via the network. The provider injects the user fingerprint data into an information access program and transfers the information access program back to the user via the network. Direct user fingerprint data is then obtained from the user and compared to the injected user fingerprint data. If there is a match, the user is enabled to use the information access program.

## BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and may be better understood by referring to the following description in conjunction with the accompanying drawings, in which like references indicate similar elements and in which:

FIG. 1 is an overview level diagram of a sample system compatible with the present invention;

FIG. 2 is a functional block diagram of a digital processing system and a sensor compatible with the present invention;

FIG. 3 is a functional block diagram of one embodiment of a networked sensor and server compatible with the present invention;

FIG. 4 is a functional block diagram of one embodiment of a wallet compatible with the present invention;

FIG. 5 is a diagram of one embodiment of a digital system compatible with the present invention;

FIG. 6 is a flowchart of a method for using fingerprints to distribute information over a network compatible with the present invention.

## DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT OF THE PRESENT INVENTION

In the following description of a preferred embodiment, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration a specific embodiment in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention. A preferred embodiment of the present invention, described below, enables a remote computer system user to execute a software application on a network file server.

In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be evident, however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to facilitate description.

In one embodiment, steps according to the present invention are embodied in machine-executable software instructions, and the present invention is carried out in a processing system by a processor executing the instructions, as will be described in greater detail below. In other embodiments, hardwired circuitry may be used in place of, or in combination with, software instructions to implement the present invention.

### Hardware Environment

FIG. 1 illustrates an overview level diagram of a sample system in which one embodiment of the present invention may be implemented. A

digital system **110** is a computing system which has the processing ability to compare a received digitized image with a database of digitized templates, and control a digital connection for receiving the digitized image. In the preferred embodiment, the digital connection is a data bus which conforms to a universal serial bus (USB) standard, as is well known to those of ordinary skill in the art. In FIG. **1**, digital system **110** is represented as a computer system. The computer system **110** includes a body **120**, which contains the processing power of the computer system **110**. Computer system **110** also includes a display **130**. The display **130** may be a liquid crystal display (LCD), cathode ray tube (CRT), or similar display mechanism. Computer system **110** includes a data entry mechanism **140**. In this instance, a keyboard **140** is illustrated. The keyboard **140** permits a user to interact with the computer system **110**. A conventional cursor control device **145** is further illustrated. The cursor control device **145** may be a mouse, trackball, pen, or similar device.

In one embodiment, sensor **150** is coupled to the computer system **110** via a cable **170**. Alternatively, sensor **150** may be coupled to computer system **110** via an infrared, radio frequency, modem, network, or any other direct or indirect digital connection.

The sensor **150** of the present invention includes a sensor platen **160**, on which a finger is placed for the fingerprint recognition. In one embodiment, cable **170** is a universal serial bus (USB) connection. It will be apparent to those of ordinary skill in the art that other digital connections may also be used. The sensor **150** may further have a connection to a power source. However, if the cable **170** is a USB connection, no such additional power connection is required as the USB connection provides power. It is to be understood that FIG. **1** is merely an illustration of one embodiment of a system on which the present

invention may be practiced. Alternate configurations, such as a portable computer 110, a digital system which does not have all of the components illustrated, or a sensor 150 having a different shape or size may also be utilized.

FIG. 2 is a functional block diagram of the digital system 210 and sensor 250 of the present invention. In one embodiment, the digital system 210 may be embodied in a computer system 110. The digital system 210 includes a temporary data storage 215, for storing data temporarily. The temporary data storage 215 may include random access memory (RAM), and various registers. Digital system 210 further includes database 220. Database 220 is for storing fingerprint templates, identification data, etc. for each individual person who is registered with that system. Comparator 225 is for comparing fingerprint data. In one embodiment, the comparator 225 is able to compare data stored in the database 220 with data stored in the temporary data storage 215. The comparator 225 has an output which determines whether or not the data provided to it match or not.

Security unit 230 is utilized to encrypt and decrypt messages sent between the digital system 210 and the sensor 250 on line 290 and to determine, maintain and use session keys. Security unit 250 is further described below. An interface 235 interacts with the user and with other programs in the digital system 210 and the sensor 250. Interface 235 may display various windows in a WINDOWS or MACINTOSH environment. Windows is a trademark of Microsoft Corporation, and Macintosh is a trademark of Apple Computers, Inc.

Card receiving unit 240 may be integral with digital system 210, or it may be attached to digital system 210 via a bus, cable, infrared, or other connection method. Card receiving unit 240 is for receiving a token,

smart card, barcode, diskette, or similar medium which may store personal information about the holder of the card, and may contain fingerprint information. The card receiving unit **240** may be utilized to verify the identity of the card holder with respect to fingerprint information stored on the card.

Registering unit **245** enables a user to register with the digital system **210**, such that the user's fingerprint identification is placed in the database **220**. The digital system **210** may further include a universal serial bus (USB) controller **205**. The universal serial bus controller **205** couples the digital system **210** with the sensor **250**, in one embodiment. Universal serial bus controller **205** provides a data conduit as well as power to sensor **250**. The functioning of the universal serial bus controller **205** may be found in more detail in the Universal Serial Bus Specification, Revision 1.0, January 15, 1996.

Sensor **250** is coupled to the digital system **210** through connection **290**. In one embodiment, the connection **290** is USB, which provides both data and power connections. Alternatively, sensor **250** may have a separate power connection.

Sensor **250** includes a data storage unit **255**. Data storage unit **255** may include RAM, registers, as well as memory. Data storage unit **255** stores intermediate values of prints, templates, sums, session keys, permanent sensor signature, and similar data.

Sensor **250** further includes a sensing mechanism **260**. The sensing mechanism **260** may include a sensor platen, on which a user can place his or her fingers for recognition. The sensing mechanism **260** may be a conventional fingerprint sensing mechanism, consisting of a light, illuminating at least one prism, which reflects the print on the sensor platen. The reflected print is received by a detector array. Alternatively,

sensing mechanism 260 may utilize other methods of sensing, including capacitive sensors.

Sensor 250 further includes a digitizer 265. Digitizer 265 digitizes images received from the sensing mechanism 260. Mechanisms which may be used to digitize an image are known in the art. In one embodiment, a conventional analog-to-digital converter is utilized.

Sensor 250 further includes a subtractor 270. Subtractor 270 is utilized to filter a digitized fingerprint image and subtract a background image from a print, as will be described below.

Security unit 275 in the sensor 250 corresponds to the security unit 230 in the digital system 210. However, it may further store the private key of the sensor, its signature, in a tamper-proof environment.

Finally, sensor 250 includes decision making unit 280. Decision making unit 280 may be utilized to make a final determination whether a fingerprint matches the print in the database 220. Decision making unit 280 may be used when digital system 210 is not secure, and strict security is necessary. The functioning of the above described components is elaborated further below.

In one embodiment, digital system 210 may be a computer system, a PCMCIA card, a portable computer, a network station and server, a palm top computer, or any other system which may be capable of processing the data required. Furthermore, the sensor 250 may be located within the digital system 210. In such a case, no duplicative memory, security units and USB controller would be required.

FIG. 3 illustrates a network in which the present invention may be utilized. Sensor 310 is coupled to host 320. Host 320 is enabled to connect to a network 330, which couples a plurality of systems 320, 340, 350 together. A server 340 contains the database which is matched to the

fingerprint received by sensor 310. Other systems 350 may be utilized for their processing power. Thus, the actual fingerprint recognition process may be distributed over a plurality of systems 320, 340, 350. Such a distributed processing may be used for accessing remote data through a network. Because neither the server 340, nor the other systems 350 are secure, for security purposes final matching may be done in the sensor 310. This would be accomplished by sending the processed data back to the sensor 310. Thus, the sensor 310 receives matched elements, and the original fingerprint. Verifying that the matched elements truly match the original fingerprint is a process which may be accomplished in the sensor 310. Thus, the sensor 310 may send out the final matched/not matched signal, thus creating a secure system over an insecure network 330.

FIG. 4 illustrates a block diagram of one embodiment of a system which combines the functionality of the sensor 250 and digital system 210 into a single unit, called a wallet 400. A wallet 400 may be implemented with different configurations of software and hardware. For example, the entire wallet 400 may reside in a smart card, or it may be implemented as a distributed system that may include a smart card, database, and matching/control software distributed over a network.

Sensing unit 410 has a sensor platen 415 on which a finger is placed. Sensing unit 410 receives the image, and passes it on to digitizer 420. Digitizer 420 digitizes the fingerprint image, and passes it on to a matching unit 425. Matching unit 425 further has access to a storage unit 430, which stores a database of templates. Matching unit 425 matches the features of the received fingerprint, to the templates in the storage unit 430. In one embodiment, such a wallet 400 belongs to one individual only, whose print is stored in the storage unit 430. The matching unit 425 passes on a yes/no decision, whether prints match, to a data flow control

unit 435. The data flow control unit 435 controls access to data stored in a user data unit 440. The data flow control unit 435 may further allow the user to upload information to the wallet 400 once the user's access to the wallet 400 is verified.

The user data unit 440 may contain such information as the user's credit card number, social security number, and identity. The user data unit 440 may further contain any information a user wishes to store in the user data unit 440. The wallet 400 further may include a control mechanism 445, such as a keyboard, mouse, trackball, touch pad, etc. The user may utilize the control mechanism 445 to add data to the wallet 400.

FIG. 5 is a diagram of one embodiment of the digital system of the present invention. Digital system 500 comprises a system bus 510 or other communication means for communicating information, and a processor 520 coupled with system bus 510 for processing information. Digital system 500 also comprises a read only memory (ROM) and/or other static storage device 535 coupled to system bus 510 for storing static information and instructions for processor 520. The digital system 500 further comprises a main memory 530, a dynamic storage device for storing information and instructions to be executed. Main memory 530 also may be used for storing temporary variables or other intermediate information during execution of instructions. In one embodiment the main memory 530 is dynamic random access memory (DRAM).

Digital system 500 further comprises a universal serial bus (USB) controller 580, a bus controller for controlling a universal serial bus (USB) 585. The USB 585 is for coupling USB devices 590 to the digital system 500. The sensor 250 may be one of the USB devices 590 coupled to the digital system 500 via the USB 585.

Digital system 500 can also be coupled via system bus 510 to a display device 550, such as a cathode ray tube (CRT) or liquid crystal display (LCD) screen, for displaying information to a user. An alphanumeric input device 555 is typically coupled to system bus 510 for communicating information and command selections to processor 520. Another type of user input device is cursor control device 560, such as a mouse, a trackball, trackpad, or cursor direction keys for communicating direction information and command selections to processor 520 and for controlling cursor movement on display device 550. Alternatively, other input devices such as a stylus or pen can be used to interact with the display. The digital system 500 may further be coupled via the system bus 510 to a network communication device 565. The network communication device 565 may be utilized to couple the digital system to other digital systems, servers, and networks.

Software Environment

The present invention provides for the use of a fingerprint to insure data integrity, data authenticity, and user verification when distributing information over a network. The present invention may be used with any type of digital information, including, but not limited to, software programs, sound or recorded music files, photographs, movies, books, documents, or any other type of digital record. The present invention may be used when information or software is sold to a user by a provider, or in other non-commercial situations such as a taxpayer viewing their social security records through the federal government.

A flowchart of a preferred method to distribute digital information over a network is shown in FIG. 6. At step 601, user fingerprint data is obtained from the user. Typically this is provided directly by the user

through the sensor **150, 250**. However, it will be recognized by one of ordinary skill in the art that user fingerprint data may be provided to the present invention by many means other than the sensor **150, 250**, such as by an encoded smart card, or by a virtual address book which stores one or more fingerprints in a file on the computer system **110**. At step **603**, the user fingerprint data is sent to the information provider via the network. To provide additional security, the user fingerprint data may optionally be encrypted by the computer system **110** with an encryption key previously distributed to the user by the provider. In one embodiment of the present invention, the user fingerprint data may be used as a cryptographic key. The concurrently filed application entitled "Cryptographic Key Generation Using Biometric Data", Serial No. _____, filed November 14, 1997, which teaches a method of generating a cryptographic key based on a fingerprint, is incorporated herein by reference.

At step **605**, the user fingerprint data is injected into an information access program. The information access program may be one of many different types of digital files, such as a software installation program, a software application program, a program for encrypting or decrypting information, or a data file such as a sound or recorded music file, a photograph, a movie, or any other type of digital record. It will be recognized by one of ordinary skill in the art that the step of injecting the user fingerprint data into the information access program may differ depending on the type of information access file without loss of generality with the present invention. For example, a software installation program may have the user fingerprint data inserted into a fixed area of the program. In another example using a data file, the user fingerprint data

may be encoded in a digital picture through the low-order bit of a group of pixels.

At step **607**, the information access program is transferred back to the user via the network. Once the user has received the information access program, the user preferably runs the program from the computer system **110**. At step **609**, the user is prompted to provide direct user fingerprint data, preferably through the use of the sensor **150, 250**. While direct fingerprint data may be requested once in the case of a software installation program, it may also be required many times, for viewing a photograph when a user uses an access program to view many digital photographs.

In one embodiment of the present invention, if software or data is being rented or otherwise provided on demand over the network, a timestamp or other tracking information may be encoded with the injected user fingerprint data. The tracking information may be used to control the number of times the software or data can be accessed by only prompting the user for the direct fingerprint data while user is authorized to access the information.

At step **611**, the information access program compares the direct user fingerprint data with the previously injected user fingerprint data. At step **613**, if the direct user fingerprint data matches that of the injected user fingerprint data, the information access program is enabled to allow the user to access the information. In the case where the information access program is a software installation program, the program will proceed to install the software on the user's system. In the case where the information access program is a software installation program or a data file, the program decompresses or unencrypts the installation program or data file so it may be viewed, heard, or otherwise used or experienced by

the user. It will be noted by one of ordinary skill in the art that a wide variety of other enablement techniques may be used with the present invention without loss of generality.

While the invention is described in terms of preferred embodiments in a specific system environment, those of ordinary skill in the art will recognize that the invention can be practiced, with modification, in other and different hardware and software environments within the spirit and scope of the appended claims.

## CLAIMS

What is claimed is:

1. A method for distributing information from a provider to a user over a network comprising the steps of:

transferring user fingerprint data to the provider via the network;

injecting the user fingerprint data into an information access program of the provider; and

transferring the information access program to the user via the network.

2. The method of claim 1 further comprising the steps of:

obtaining direct user fingerprint data from the user;

comparing the direct user fingerprint data with the user fingerprint data; and

enabling the information access program to access information if there is a match between the direct user fingerprint data and the user fingerprint data.

3. The method of claim 2 wherein the step of obtaining direct user fingerprint data comprises the step of obtaining a live fingerprint from the user.

4. The method of claim 2 wherein the step of obtaining direct user fingerprint data comprises the step of obtaining fingerprint data from a virtual address book.

5. The method of claim 2 wherein the step of obtaining direct user fingerprint data comprises the step of obtaining fingerprint data from a smart card.

6. The method of claim 2 wherein the step of enabling the information access program to access information comprises the step of decrypting the information access program previously encrypted with the injected user fingerprint data as a cryptographic key.

7. The method of claim 2 further comprising the steps of:

transferring second user fingerprint data to the provider via the network; and

injecting the second user fingerprint data into the information access program.

8. The method of claim 7 further comprising the steps of:

comparing the direct user fingerprint data with the user fingerprint data and the second user fingerprint data; and

enabling the information access program to access information if there is a match between the direct user fingerprint data and the second user fingerprint data.

9. The method of claim 1 further comprising the steps of:

encrypting a data file using the user fingerprint data as a cryptographic key;

injecting the user fingerprint data into the data file; and

transferring the data file to the user via the network.

10. An apparatus for distributing information from a provider to a user over a network, the apparatus comprising:

a digital computer having input means for allowing the entering of user fingerprint data;

means coupled to the network and the digital computer for transferring user fingerprint data to the provider via the network;

means coupled to the network for injecting the user fingerprint data into an information access program of the provider; and

means coupled to the network for transferring the information access program to the user via the network.

11. The apparatus of claim 10 further comprising:

means operated by the digital computer for obtaining direct user fingerprint data from the user;

means operated by the digital computer for comparing the direct user fingerprint data with the user fingerprint data; and

means operated by the digital computer for enabling the information access program to access information if there is a match between the direct user fingerprint data and the user fingerprint data.

12. The apparatus of claim 11 wherein the means operated by the digital computer for obtaining direct user fingerprint data comprises means for obtaining a live fingerprint from the user.

13. The apparatus of claim 11 wherein the means operated by the digital computer for obtaining direct user fingerprint data comprises means for obtaining fingerprint data from a virtual address book.

14. The apparatus of claim 11 wherein the means operated by the digital computer for obtaining direct user fingerprint data comprises means for obtaining fingerprint data from a smart card.

15. The apparatus of claim 11 wherein the means operated by the digital computer for enabling the information access program to access information comprises means for decrypting the information access program previously encrypted with the injected user fingerprint data as a cryptographic key.

16. The apparatus of claim 11 further comprising:

means operated by the digital computer for transferring second user fingerprint data to the provider via the network; and

means coupled to the network for injecting the second user fingerprint data into the information access program.

17. The apparatus of claim 16 further comprising:

means operated by the digital computer for comparing the direct user fingerprint data with the user fingerprint data and the second user fingerprint data; and

means operated by the digital computer for enabling the information access program to access information if there is a match between the direct user fingerprint data and the second user fingerprint data.

18. The apparatus of claim 10 further comprising:

means coupled to the network for encrypting a data file using the user fingerprint data as a cryptographic key;

means coupled to the network for injecting the user fingerprint data into the data file; and

means coupled to the network for transferring the data file to the user via the network.

19. An article of manufacture for use in a computer system for distributing information from a provider to a user over a network, the computer having a keyboard, pointing device, visual display, and data storage device, the article of manufacture comprising a computer usable medium having computer readable program code means embodied in the medium, the program code means including:

computer readable program code means embodied in the computer usable medium for causing a computer to transfer user fingerprint data to the provider via the network;

computer readable program code means embodied in the computer usable medium for causing a computer to inject the user fingerprint data into an information access program of the provider; and

computer readable program code means embodied in the computer usable medium for causing a computer to transfer the information access program to the user via the network.

20. The article of manufacture of claim 19 further comprising:

computer readable program code means embodied in the computer usable medium for causing a computer to obtain direct user fingerprint data from the user;

computer readable program code means embodied in the computer usable medium for causing a computer to compare the direct user fingerprint data with the user fingerprint data; and

computer readable program code means embodied in the computer usable medium for causing a computer to enable the information access program to access information if there is a match between the direct user fingerprint data and the user fingerprint data.

21. The article of manufacture of claim 20 wherein the means for causing a computer to obtain direct user fingerprint data comprises means embodied in the computer usable medium for causing a computer to obtain a live fingerprint from the user.

22. The article of manufacture of claim 20 wherein the means for causing a computer to obtain direct user fingerprint data comprises means embodied in the computer usable medium for causing a computer to obtain fingerprint data from a virtual address book.

23. The article of manufacture of claim 20 wherein the means for causing a computer to obtain direct user fingerprint data comprises means embodied in the computer usable medium for causing a computer to obtain fingerprint data from a smart card.

24. The article of manufacture of claim 20 wherein the means for causing a computer to enable the information access program to access information comprises means embodied in the computer usable medium for causing a computer to decrypt the information access program previously encrypted with the injected user fingerprint data as a cryptographic key.

25. The article of manufacture of claim 20 further comprising:

means embodied in the computer usable medium for causing a computer to transfer second user fingerprint data to the provider via the network; and

means embodied in the computer usable medium for causing a computer to inject the second user fingerprint data into the information access program.

26. The article of manufacture of claim 25 further comprising:

means embodied in the computer usable medium for causing a computer to compare the direct user fingerprint data with the user fingerprint data and the second user fingerprint data; and

means embodied in the computer usable medium for causing a computer to enable the information access program to access information if there is a match between the direct user fingerprint data and the second user fingerprint data.

27. The article of manufacture of claim 1 further comprising:

means embodied in the computer usable medium for causing a computer to encrypt a data file using the user fingerprint data as a cryptographic key;

means embodied in the computer usable medium for causing a computer to inject the user fingerprint data into the data file; and

means embodied in the computer usable medium for causing a computer to transfer the data file to the user via the network.

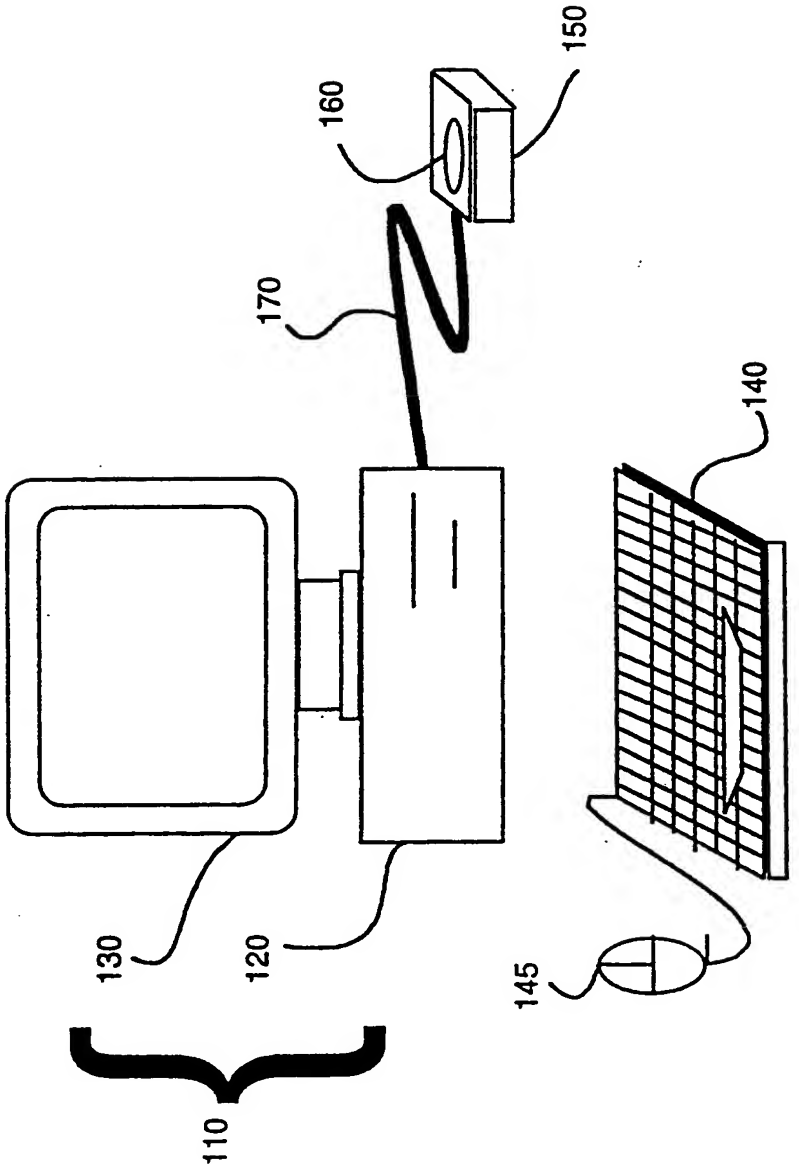



Fig. 1

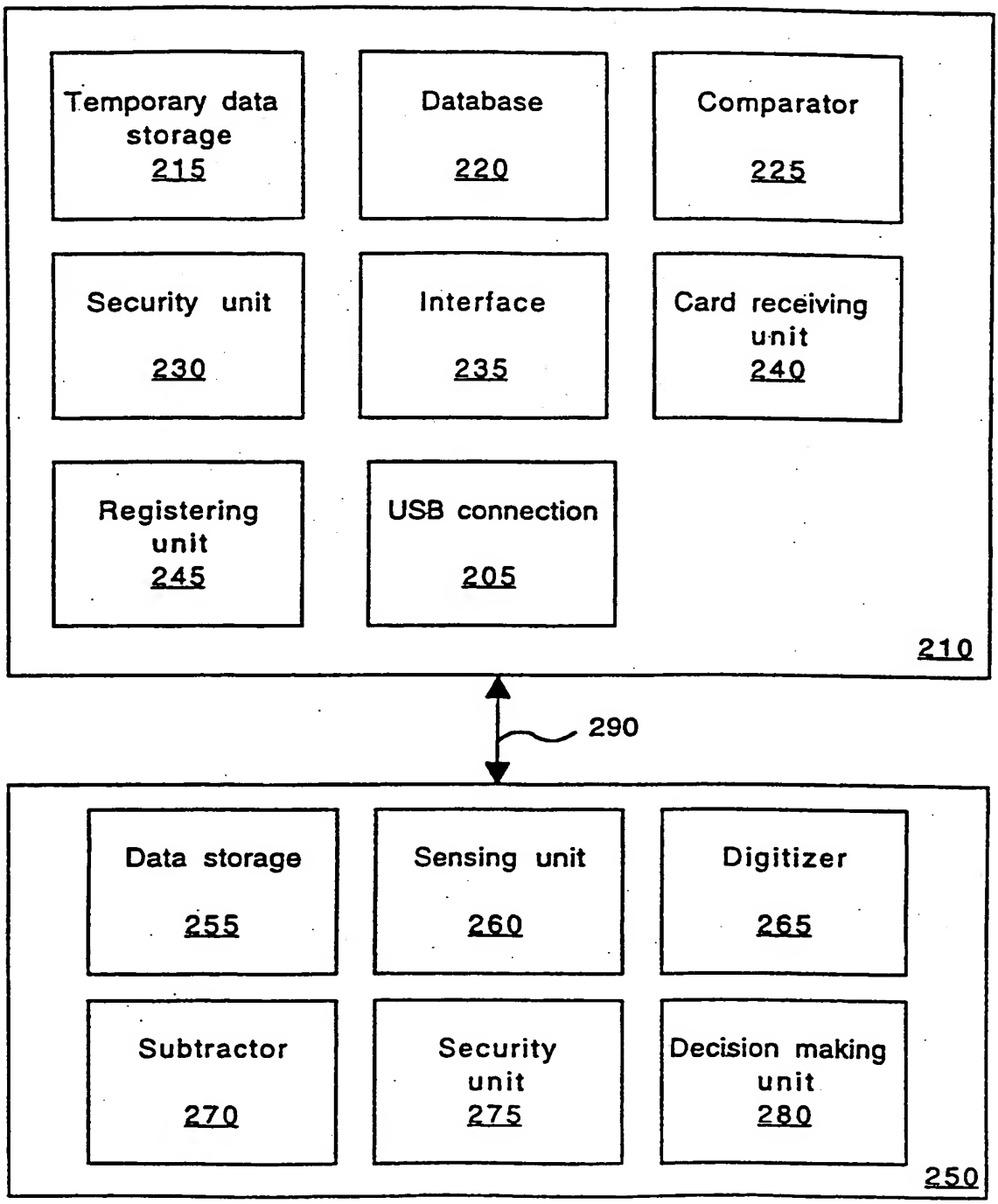



Fig. 2

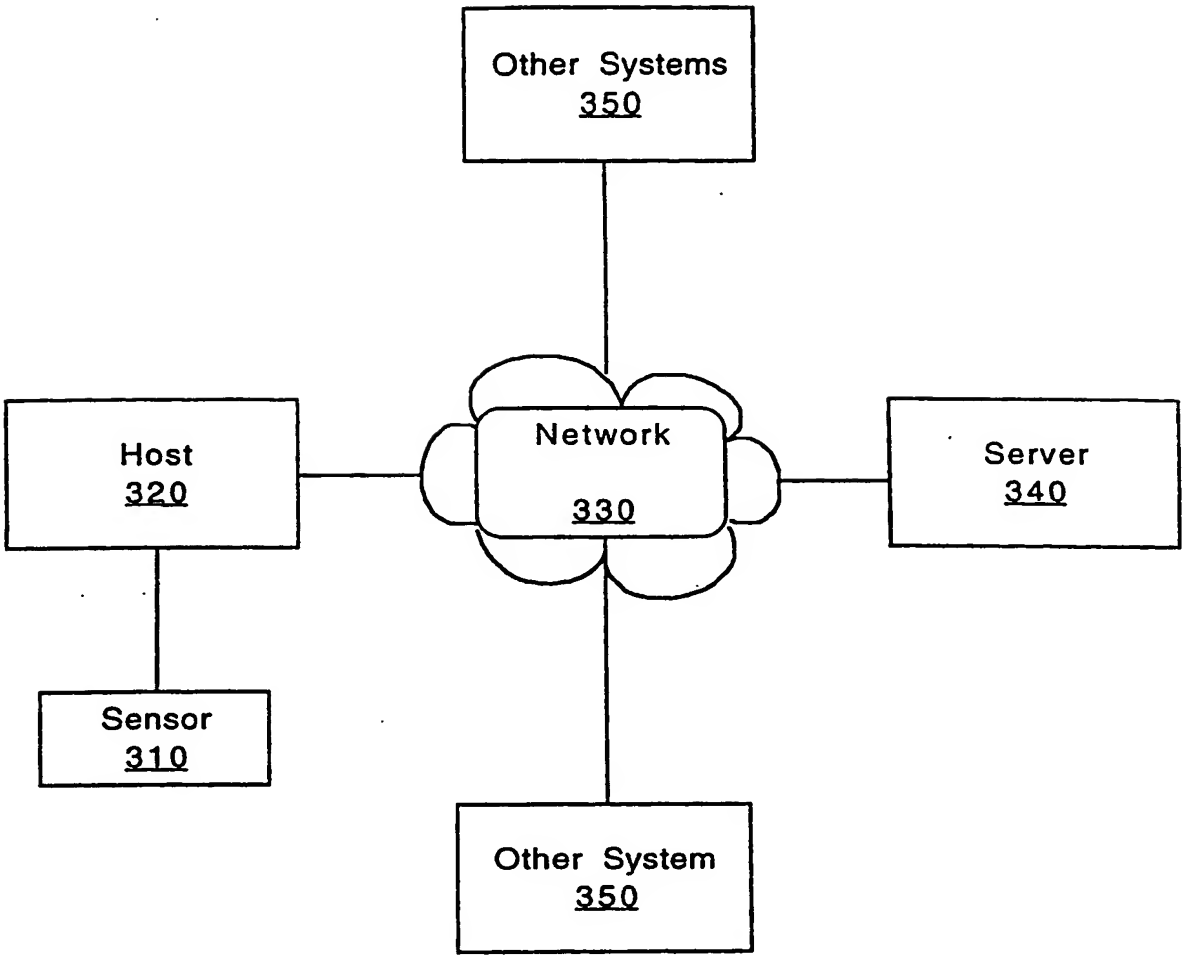

Other Systems
350
Network
330
Host
320
Server
340
Sensor
310
Other System
350

Fig. 3

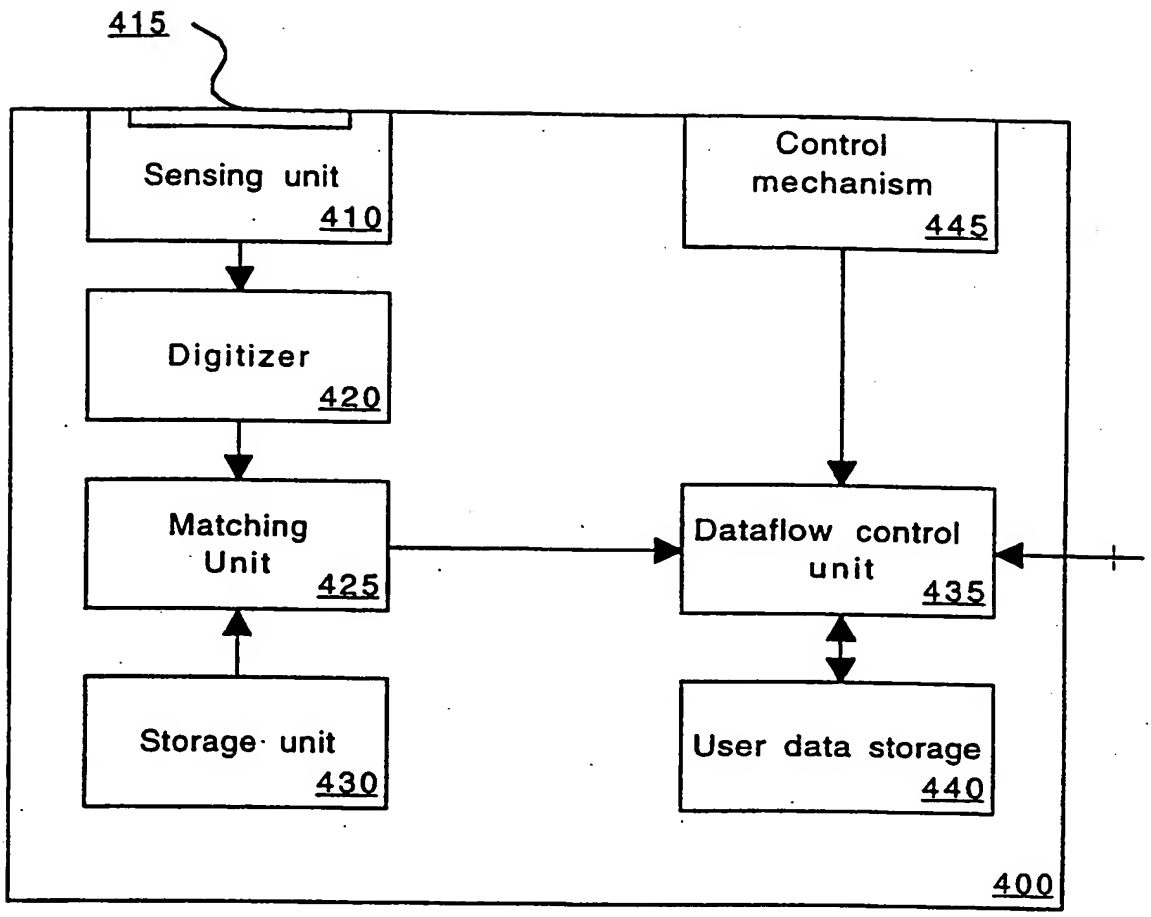

415
Sensing unit
410
Digitizer
420
Matching
Unit
425
Storage unit
430
Control
mechanism
445
Dataflow control
unit
435
User data storage
440
400

Fig. 4

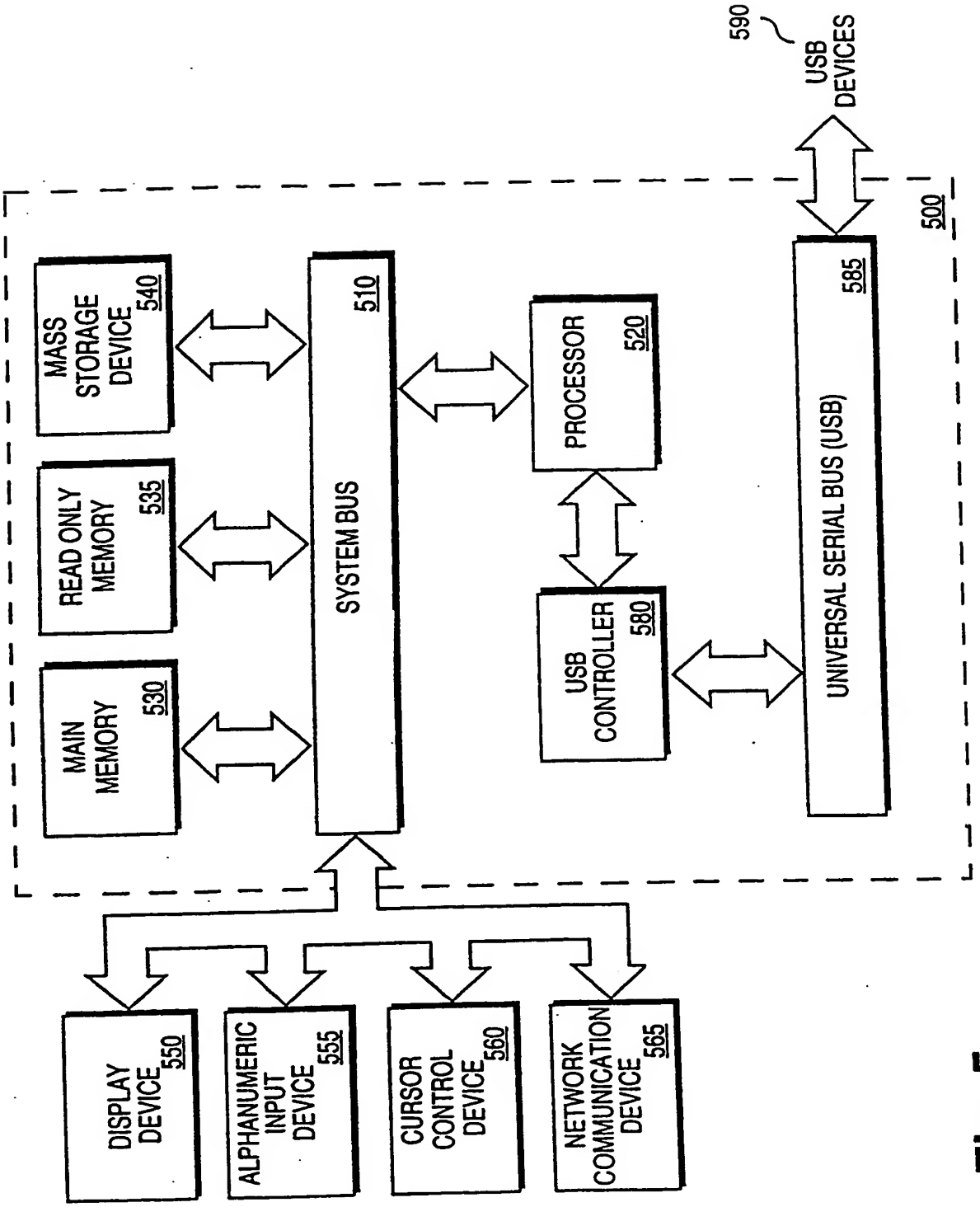

590
USB DEVICES
500
MASS STORAGE DEVICE 540
READ ONLY MEMORY 535
MAIN MEMORY 530
SYSTEM BUS 510
PROCESSOR 520
USB CONTROLLER 580
UNIVERSAL SERIAL BUS (USB) 585
DISPLAY DEVICE 550
ALPHANUMERIC INPUT DEVICE 555
CURSOR CONTROL DEVICE 560
NETWORK COMMUNICATION DEVICE 565

Fig. 5

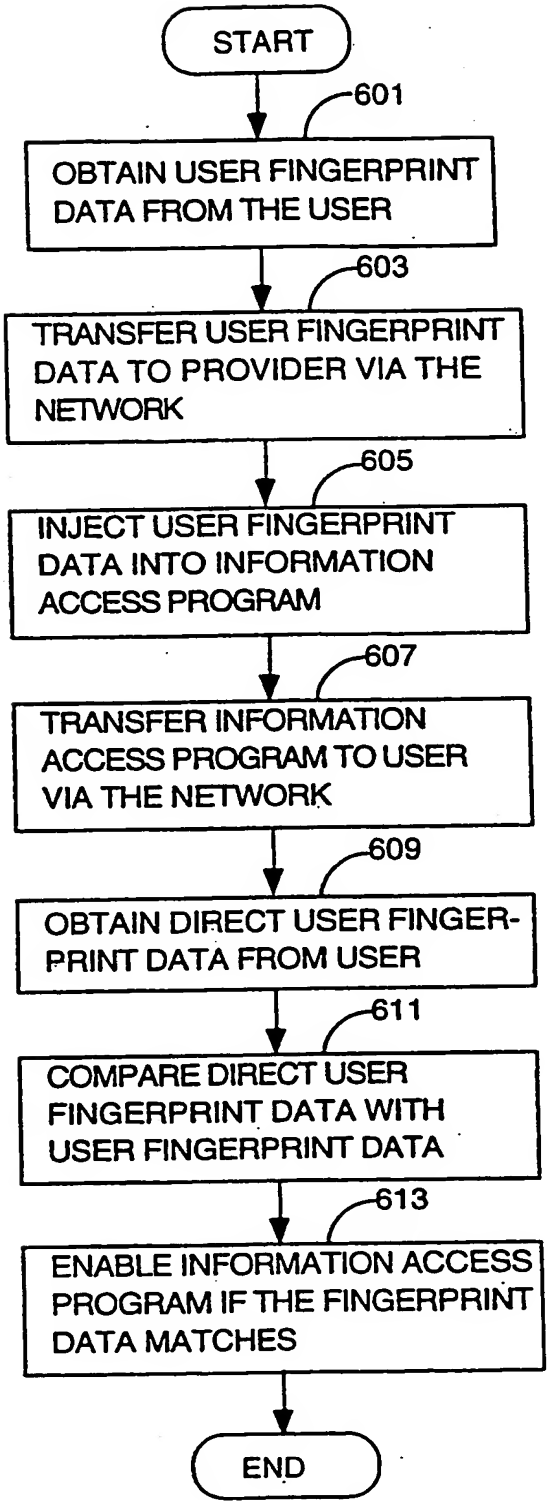

START
601
OBTAIN USER FINGERPRINT DATA FROM THE USER
603
TRANSFER USER FINGERPRINT DATA TO PROVIDER VIA THE NETWORK
605
INJECT USER FINGERPRINT DATA INTO INFORMATION ACCESS PROGRAM
607
TRANSFER INFORMATION ACCESS PROGRAM TO USER VIA THE NETWORK
609
OBTAIN DIRECT USER FINGER-PRINT DATA FROM USER
611
COMPARE DIRECT USER FINGERPRINT DATA WITH USER FINGERPRINT DATA
613
ENABLE INFORMATION ACCESS PROGRAM IF THE FINGERPRINT DATA MATCHES
END

FIG. 6

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/23328

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(6) :H04L 9/32
US CL :380/4, 23; 382/124
According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/4, 23, 24, 25, 44; 382/124

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS: biometric, encrypted software, access control program

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 5,577,120 A (PENZIAS) 19 NOVEMBER 1996, col. 2, lines 36-60. | 1-27 |
| Y | US 5,559,885 A (DREXLER et al) 24 SEPTEMBER 1996, col. 5, lines 11-34. | 1-27 |
| A | US 5,509,074 A (CHOUDHURY et al) 16 APRIL 1996, col. 2, lines 48-64. | 1-27 |
| Y | US 5,509,070 A (SCHULL) 16 APRIL 1996, col. 5, lines 20-46 and col. 17, lines 20-30. | 1-27 |
| Y | US 5,337,357 A (CHOU et al) 09 AUGUST 1994, col. 2, lines 40-56. | 1-27 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | | | |
|---|---|---|---|
| * | Special categories of cited documents: | "T" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| "A" | document defining the general state of the art which is not considered to be of particular relevance | "X" | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| "E" | earlier document published on or after the international filing date | "Y" | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" | document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" | document member of the same patent family |
| "O" | document referring to an oral disclosure, use, exhibition or other means | | |
| "P" | document published prior to the international filing date but later than the priority date claimed | | |

Date of the actual completion of the international search
07 JANUARY 1999

Date of mailing of the international search report
31 MAR 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
GILBERTO BARRÓN JR. Joni Hill
Telephone No. (703) 305-1830

Form PCT/ISA/210 (second sheet)(July 1992)*